					Insert Registered Legal Entity Name Here							
Document number: P25					Document Title: **Application Security Requirements Policy**							
Version: 1.0		Effective Date: 01.01.2025			Document Owner:							
X	Policy		Standard		Procedure		Form		Register		Other	

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations

Standard/Regulation	Clause/Article	Comment
ISO/IEC 27001:2022	Clause 8	—
ISO/IEC 27002:2022	Controls 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
EU GDPR	Articles 25, 32	—
EU NIS2	Articles 21(2)(f), 23	—
EU DORA	Articles 9, 11	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Purpose

1.1 This policy defines mandatory application security requirements for software developed, acquired, integrated, or deployed by the organization. It ensures that all applications are designed, implemented, and maintained in accordance with secure development principles, regulatory obligations, and the organization's risk appetite.

1.2 This policy mandates the integration of security throughout the application lifecycle, including user authentication, data handling, interface protection, and secure interaction with application programming interfaces (APIs) and services.

1.3 By adopting this policy, the organization aims to prevent the introduction of software vulnerabilities, protect sensitive data, and ensure traceability and resilience against exploitation and abuse.

2. Scope

2.1 This policy applies to all:

2.1.1 Internally developed and externally sourced applications, including SaaS solutions and custom-built tools

2.1.2 Applications that support critical business operations, customer access, or the processing of regulated data

2.1.3 Development, DevOps, QA, product, and security teams

2.1.4 Third-party providers, software vendors, and integration partners with access to organizational applications or application programming interfaces (APIs)

2.2 It applies across all environments, including development, testing, staging, production, and disaster recovery, regardless of whether hosted on-premises, in private data centers, or in public cloud environments.

3. Objectives

3.1 Define baseline functional and non-functional security requirements to be met by all applications, regardless of development methodology or technology stack.

3.2 Ensure the implementation of application-layer protections, including input validation, output encoding, error handling, and session security.

3.3 Require the secure implementation of authentication, authorization, and access control mechanisms aligned with the organization's identity and access management policies.

3.4 Mandate secure interaction with application programming interfaces (APIs), web interfaces, and third-party components using approved hardware, protocols, and security controls.

3.5 Enable early detection and mitigation of vulnerabilities through static and dynamic analysis, code review, and threat modeling.

3.6 Protect sensitive data in compliance with regulatory requirements by enforcing encryption, data classification, and retention schedule requirements.

3.7 Ensure continuous validation of the application security posture following deployment through testing, monitoring, threat detection, and audit readiness activities.

4. Roles and Responsibilities

4.1 Chief Information Security Officer (CISO)

4.1.1 Owns this policy and ensures alignment with the organization's information security strategy and risk posture.

4.1.2 Approves application security requirements and enforces mandatory controls across development and procurement functions.

4.2 Application Security Lead / DevSecOps Manager

4.2.1 Defines baseline security controls and testing methodologies for application components.

4.2.2 Oversees the secure integration of tools such as SAST, DAST, IAST, and SCA into the software delivery pipeline.

4.2.3 Maintains the Application Security Requirements Checklist and validation criteria.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Review and Update Requirements

9.1 This policy must be reviewed annually, or more frequently in response to:

9.1.1 Critical vulnerability disclosures affecting commonly used frameworks or dependencies

9.1.2 Changes to regulatory obligations relating to application security, such as NIS2 or DORA

9.1.3 Major changes to the organization's software development practices, tooling, or cloud architecture

9.1.4 Findings from internal audits or external penetration tests

9.2 The review shall be led by the Application Security Lead in coordination with the CISO, DevOps Engineering, Legal and Compliance, Procurement, and QA leadership.

9.3 All revisions must be version-controlled in the ISMS Document Control Register and communicated to all affected development and product teams.

9.4 Superseded versions must be retained in the archive for no less than three years to support traceability, auditability, and data breach investigations.

10. Related Policies and Linkages

10.1 P1 – Information Security Policy. Establishes the foundation for protecting systems and data, under which application-level controls are required to prevent unauthorized access, data leakage, and exploitation.

10.2 P4 – Access Control Policy. Defines the identity and session management standards that must be enforced by all applications, including strong authentication, least privilege, and access review requirements.

10.3 P5 – Change Management Policy. Governs the promotion of application code and configurations into production environments, ensuring unauthorized or untested changes are blocked.

10.4 P17 – Data Protection and Privacy Policy. Requires applications to implement privacy by design and to ensure the lawful handling, encryption, and retention of personal and sensitive data across all environments.

10.5 P24 – Secure Development Policy. Provides the broader framework for embedding security into the SDLC, while this policy defines the specific requirements and technical controls to be implemented at the application layer.

10.6 P30 – Incident Response Policy. Mandates the structured handling of application security incidents, including vulnerabilities identified after deployment or during penetration testing, and defines escalation, containment, and recovery procedures.

11. Reference Standards and Frameworks

11.1 ISO/IEC 27001:2022

11.1.1 Clause 8.1 – Operational Planning and Control: Requires application security to be embedded into processes and systems to ensure confidentiality, integrity, and availability.

11.2 ISO/IEC 27002:2022

11.2.1 Controls 8.25–8.26: Detail expectations for application security, including secure coding practices, threat modeling, architectural controls, and third-party software validation.

11.2.2 Annex A Control 8.25 – Secure Development Life Cycle: Requires security integration across the application lifecycle.

11.2.3 Annex A Control 8.26 – Application Security Requirements: Requires the definition and enforcement of technical controls to protect applications against misuse and compromise.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Developer Security Testing and Evaluation: Requires static analysis, dynamic analysis, and penetration testing during development.

11.3.2 SA-15 – Development Process, Standards, and Tools: Establishes formal standards for secure application development.

11.3.3 SI-10 – Information Input Validation: Requires control mechanisms to prevent injection and parsing attacks.

11.4 EU GDPR (2016/679)

11.4.1 Article 25 – Data Protection by Design and by Default: Requires the integration of data protection and privacy into application logic and workflows.

11.4.2 Article 32 – Security of Processing: Requires appropriate technical measures, such as input validation, encryption, and secure access controls.

11.5 EU NIS2 Directive (2022/2555)

11.5.1 Article 21(2)(f): Requires vulnerability handling and secure application lifecycle practices for essential and important entities.

11.5.2 Article 23 – Reporting of Security Incidents: Requires application-layer logging, monitoring, and threat detection capabilities to detect and report significant incidents.

11.6 EU DORA (2022/2554)

11.6.1 Article 9 – ICT Risk Management: Requires financial entities to ensure applications are secure, tested, and resilient against cyberattacks.

11.6.2 Article 11 – Testing of ICT Tools: Supports periodic penetration testing and red teaming of critical applications and services.

11.7 COBIT 2019

11.7.1 BAI03 – Manage Solutions Identification and Build: Establishes design and control requirements during application development.

11.7.2 BAI09 – Manage Applications: Emphasizes the secure maintenance, monitoring, and enhancement of live applications.

11.7.3 DSS05 – Manage Security Services: Links application protection to broader organizational security operations and controls.